CENTER FOR DEMOCRACY & TECHNOLOGY

September 29, 2016

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th St. SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

On Tuesday, September 27, Chris Calabrese and Natasha Duarte of the Center for Democracy & Technology met with Gigi Sohn and Stephanie Weiner of the Chairman's Office and Matthew DelNero and Lisa Hone of the Wireline Bureau to discuss matters in the above referenced proceeding. During the meeting, CDT shared its views on several aspects of the rulemaking, including de-identification, the categorization of data as sensitive or non-sensitive, pay-for-privacy models, and data security and data breach standards.

I. De-identification

CDT advocated for clear definitions and standards for the de-identification of customer data. Although Section 222 exempts "aggregate customer information" from its privacy mandate,[1] the statute requires such aggregate information to be de-identified.[2] Because aggregation does not always result in de-identification, it is imperative that the FCC's rules explicitly require de-identification of information as a prerequisite to the use and sharing of aggregate data. The FCC should require that aggregate data is not reasonably linkable to any individual or device and should place the burden upon broadband providers to monitor re-identification efforts after the information is disclosed.

De-identification alone should not exempt data from the FCC's choice framework. Section 222's exemption applies to data that is both aggregate and de-identified. The removal of individual identifiers from a customer's information, without more, does not satisfy this definition because it permits easy re-identification by third parties, who may have access to information that *is* linked to individuals. For example, if a broadband company shared a customer's video streaming history with identifying information removed, a video streaming service, such as Netflix, could re-identify the customer by comparing the de-identified streaming history with its own individually identifiable

[1] 47 U.S.C. § 222(c)(3).
[2] § 222(h)(2).

customer records. By contrast, if the broadband provider aggregated such data to count the number of times a particular video was viewed, it would be much more difficult if not impossible to identify individual viewers from that aggregate data point. Aggregation *and* de-identification are both crucial steps required to obscure the linkability of information to any individual or device. Thus, a carve-out for data that is "de-identified" but not aggregate would violate the statute, as would a carve-out for aggregate but not de-identified data.

In addition, there may be some information that simply can't be de-identified. For example, specific geolocation information may be stripped of all identifying information but still be identifiable because of its very nature – if it is known where an individual sleeps at night and where she spends her working hours, it is trivial to use that information to re-identify that individual and then gain a historical record of all her movements.

II. Categorizing data as sensitive and non-sensitive

CDT reiterated its position that offering one level of protection (in this case, opt-in) for "sensitive" information and another level of protection (opt-out) for other information would be impractical and would negate consumer choice. The sensitivity of information is highly subjective and context-dependent. Information that is not considered sensitive to some may be considered highly sensitive to others—especially vulnerable minority groups. Even seemingly innocuous information such as IP addresses can sometimes reveal where a person lives,[3] which can be used to infer characteristics such as race and income level.[4]

Moreover, a single piece of data may seem non-sensitive on its own but reveal sensitive information when combined with other data points. "Non-sensitive" information can be a lynchpin in a broader system of profiling. One example of this can be seen by looking at information that is often viewed as public — the name and physical address of a customer plus his or her IP address.[5] Treating only those types of information as less sensitive could result in a significant privacy invasion because the information would facilitate a connection with other, existing pools of information.

---

[3] Alix Jean-Pharuns, *Keep Calm and Keep Assigning IP Addresses*, MOTHERBOARD (July 10, 2015), http://motherboard.vice.com/read/keep-calm-and-keep-assigning-ip-addresses.

[4] Alethea Lange & Rena Coen, *How Does the Internet Know Your Race?*, CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 7, 2016), https://cdt.org/blog/how-does-the-internet-know-your-race/.

[5] BIAS providers have long shared name and address information as part of creating a directory of users in the telephone context. Similarly, IP address is often viewed as less sensitive because it is shared with every website as part of web browsing.

In practice this would work in the following way. At least one large ISP, Verizon, already owns a large internet adverting network, AOL. AOL monitors web browsing across the web (not just of AOL users) and uses that information to serve targeted ads. As such, AOL has detailed web browsing information (including IP address) but not necessarily knowledge of who an individual user is.[6] On the other side of the equation, data brokers such as Acxiom sell detailed profiles of an individual's purchasing habits, property records and other information derived from offline sources.[7] This information is almost always tied to name and physical address. Given this information ecosystem, name and physical address plus IP address becomes the connective tissue that links these two huge pools of data together. This connection would allow a persistent record to be created and maintained on an individual's entire online and offline life with only these two seemingly innocuous pieces of information.

Under a regime that does not treat all personal information as sensitive, the customer would only be able break this connection if they affirmatively opt out of the sharing of IP address and name/address. While certainly possible, it puts a tremendous burden on the consumer, requiring them to understand a vast digital ecosystem and a complicated privacy notice. Instead, the rules should protect customer choice by requiring clear notice and affirmative consent for the use of customer proprietary information as defined in the NPRM. This framework still allows broadband providers to offer attractive services to customers who consent to certain uses of their information.

III. Pay-for-privacy

CDT argued that the FCC should prohibit BIAS providers from coercing customers into consenting to the use and sharing of their personal information in exchange for affordable service. Pricing models that make service unaffordable for customers who do not opt in to data sharing should be viewed as unconscionable and as effectively conditioning service on the relinquishment of privacy. This argument is further delineated in our May 27, 2016 comments. We also urged the Commission to pay special attention to the need for transparency around the costs and benefits to any provider of offering any type of pay-for-privacy model. Particularly important would be information regarding how many customers chose the privacy protective program. If the program has little or no uptake, that might be

[6] Note this information does not come from the provision on broadband service and hence is outside of the scope of the proposed rule and its protections.

[7] Staff of S. Comm. On Commerce, Science, and Transportation, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes (Dec. 18, 2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

evidence to the Commission that the program is priced in such a way as to coerce customers to accept a less privacy protective approach.

IV. Data security

CDT expressed its support for a reasonableness standard for protecting the security of customer data, as long as the standard is upheld through enforcement actions that hold companies accountable and provide guidance regarding what is reasonable. Providing companies with a checklist of requirements for securing data would be ineffective given the fast-changing nature of data security and hacking technology. CDT also expressed its support for clear data breach standards.

Respectfully submitted,

Chris Calabrese
VP of Policy, Center for Democracy & Technology
1401 K Street NW Suite 200
Washington, DC 20005
202.637.9800